12-05-07

IDW 3624

PTO/SB/21 (11-07)
Approved for use through 11/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	09/250,340
Filing Date	February 16, 1999
First Named Inventor	Yik Hei SIA
Art Unit	3624
Examiner Name	Kazimi, Hani M.
Attorney Docket Number	212/656

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☑ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

Certified copy of application number PI9800664

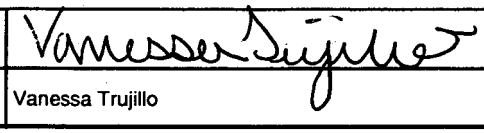
Express Mail No. EV801363105US
Date of Mailing: December 3, 2007

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Crockett & Crockett		
Signature			
Printed name	K. David Crockett, Esq.		
Date	December 3, 2007	Reg. No.	34,311

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Vanessa Trujillo	Date	December 3, 2007

(Diperbadankan)

Aras 27, 30 dan 32, Menara Dayabumi, Jalan Sultan Hishamuddin, 50623 Kuala Lumpur
Tel : 603-2274 2100 Fax : 603-2274 1332 Website : www.myipo.gov.my

To:

MS. SIA YIK HEI
44, JALAN INDAH 1/23,
TAMAN BUKIT INDAH,
81200 JOHOR BAHRU,
JOHOR
MALAYSIA.

PATENT APPLICATION NO: PI 9800 0664

This is to certify that annexed hereto is a true copy from the records of the Patent Registration Office, Malaysia of the application as originally filed which is identified therein.

By authority of the
REGISTRAR OF PATENTS

ROZANAH MISKAN
(CERTIFYING OFFICER)
20-Jun-2007
rozanah@myipo.gov.my
Tel: 03-22632124

KEMENTERIAN PERDAGANGAN DALAM NEGERI
DAN HAL EHWAL PENGGUNA MALAYSIA
BAHAGIAN HARTA INTELEK,
TINGKAT 22,
MENARA MAYBANK,
100, JALAN TUN PERAK,
50050 KUALA LUMPUR.
Ministry of Domestic Trade and Consumer Affairs Malaysia
Intellectual Property Division.

Telefon: 03-2329955
Fax : 03-2012618

CERTIFICATE OF FILING

APPLICANT	:	SIA YIK HEI
APPLICATION NO	:	PI 9800664
REQUEST RECEIVED ON	:	17/02/1998
FILING DATE	:	17/02/1998
AGENT'S/APPLICANT'S FILE REF.	:	DM/RAG/PAT/02,117/KL

Please find attached, a copy of the Request Form relating to the above application, with the filing date and application number marked thereon in accordance with Regulation 25(1).

Date : 30/04/1998

.....

(HASNON BT ALANG MOHD RASHID)
for Registrar of Patents

To : FOONG SEET FUN,
DREWMARKS PATENTS AND DESIGNS (M) SDN BHD,
9TH FLOOR, BGN GETAH ASLI ,
148, JALAN AMPANG,
50450 KUALA LUMPUR,
MALAYSIA.

FF 09

Pat... Form No. 1
PATENTS ACT 1983

REQUEST FOR GRANT OF PATENT
(Regulation 7(1))

To : The Registrar of Patents
Patent Registration Office
Kuala Lumpur
Malaysia

For Offcial Use

APPLICATION NO : PI 9800664

Filing Date : 17 FEB 1998

Request received on : 17 FEB 1998

Fee received on : 17 FEB 1998

Amount : RM 440.

*Cheque/Postal Order/Money Order/Draft/Cash No.:

CASH.

Date of mailing :

Please submit this Form in duplicate.

~~Applicant's~~ Agent's file reference

DM/RAG/PAT/02,117/KL

THE APPLICANT(S) REQUEST(S) THE GRANT OF A PATENT IN RESPECT OF THE FOLLOWING PARTICULARS :

I. TITLE OF INVENTION : IMPROVEMENTS IN CODE BASED ACCESS SYSTEMS

II. APPLICANT(S) (the data concerning each applicant must appear in this box or, if the space is insufficient, in the space below)

Name : SIA YIK HEI

I.C./Passport No. :

Address : 73, C.F. PARK, P.O. BOX 1941, 97010 BINTULU,
SARAWAK, MALAYSIA.

Address for service in Malaysia : Roshayati Abdul Ghani/Zaharizan Ahmed Meah/Foong Seet Fun
c/o Drewmarks Patents & Designs (Malaysia) Sdn. Bhd.
9th floor Bangunan Getah Asli (Menara), 148 Jalan Ampang, 50450 Kuala Lumpur, Malaysia

Nationality : MALAYSIAN

*Permanent residence or principal place of business

SAME AS ABOVE

Telephone Number *(if any)* : (03) 262-2522

Fax Number *(if any)* : (03) 262-2804

DITERIMA 17 FEB 1998 Harta Intelek

Additional Information (if any)

III. INVENTOR

Applicant is the inventor(s) Yes [X] No [ ]

If the applicant is not the inventor(s) :

Name(s) and address(es) of inventor(s) :

NAME ADDRESS

A statement justifying the applicant's right to the patent accompanies this Form :

Yes [ ] No [X]

Additional Information (if any)

IV. AGENT OR REPRESENTATIVE

Applicant has appointed a patent agent in accompanying Form No. 17 Yes [X] No [ ]

Agent's Registration No. : PA/91/0025 / PA/95/0062 / PA/97/0068

Applicants have appointed - to be their common representatives.

V. DIVISIONAL APPLICATION

This application is a divisional application [ ]

The benefit of the filing date [ ] priority date [ ]

of the initial application is claimed in as much as the subject matter of the present application is contained in the initial application identified below :

Initial Application No. :

Date of filing of initial application :

9800664

VI. DISCLOSURES TO BE DISREGARDED FOR PRIOR ART PURPOSES

Additional information is contained in supplemental box :

(a) Disclosure was due to acts of applicant or his predecessor in title ☐

Date of disclosure : _____

(b) Disclosure was due to abuse of rights of applicant or his predecessor in title ☐

Date of disclosure : _____

A statement specifying in more detail the facts concerning the disclosure accompanies this Form

Yes ☐

No ☐

Additional Information (if any)

VII. PRIORITY CLAIM (if any)

The priority of an earlier application is claimed as follows :

Country (if the earlier application is a regional or international application, indicate the office with which it is filed) :

_____

Filing Date : _____

Application No. : _____

Symbol of the International Patent Classification :

If not yet allocated, please tick ☐

The priority of more than one earlier application is claimed.

Yes ☐ No ☒ X

The certified copy of the earlier application(s) accompanies this Form :

Yes ☐ No ☒ X

If No, it will be furnished by _____ (date)

Additional Information (if any)

VII CHECK LIST

A. This application contains the following :

1. request		sheets
2. description	17	sheets
3. claim	5	sheets
4. abstract	1	sheets
5. drawings	5	sheets
Total	28	sheets

B. This Form, as filed, is accompanied by the items checked below :

(a) signed Form No. 17	X
(b) declaration that inventor does not wish to be named in the patent	
(c) statement justifying applicant's right to the patent	
(d) statement that certain disclosure he disregarded	
(e) priority document (certified copy of earlier application)	
(f) cash, ~~cheque, money order, banker's draft or postal order~~ for the payment of application fee	X
(g) other documents (specify)	

IX.

SIGNATURE _____ 17 FEB 1998

FOONG SEET FUN (Applicant/Agent) *(Date)*

If Agent, indicate Agent's Registration No. : PA/97/0068

For Offcial Use

1. Date application received : _____

2. Date of receipt of correction, later filed papers or drawings completing the application :

_____

** Delete whichever does not apply.*

*** Type name under signature and delete whichever does not apply*

9800664

IMPROVEMENTS IN CODE BASED ACCESS SYSTEMS

Field of the Inventions

The present invention relates to improvements in code based access systems.

Background of the Inventions

Systems in which transactions or connections between two or more parts or stations of the system are conducted or established by means of an access code are known. Such systems include computer terminals wherein the access code is a password, bank terminals such as ATM machines wherein the access code is a personal identification number (PIN) and communications terminals such as mobile telephones wherein the access code is an electronic serial number (ESN). Typically the access code is provided by a user to an accessing part or station of the system and is verified against a duplicate version of the access code available to an accessed part or station of the system, before an authority to perform the transaction or to establish the connection between the stations or parts is given. US 5 355 413 by Ohno disclosed a system in which authentication is performed without an authentication code or an address being transmitted directly between the two devices to assure the security of the authentication operation. Said system being programmed to re-use an authentication code 100 times before it is replaced by a new code comprising random numbers. It also disclosed a method of selecting codes based on a formula or algorithm, for security reasons said codes being used with algorithm encryption before transmission.

A disadvantage of such systems is that the security of future transactions or connections becomes seriously compromised if the access code is detected by or otherwise becomes known to unauthorised persons i.e. Persons other than the person or persons authorised to perform the transactions or establish the connection.

An object of the present invention is to provide a code based access system which alleviates the disadvantages of the prior art or at least provides the public with a choice.

Summary

To this end the present invention provides a system including at least two parts or stations wherein a transaction or connection between any two or more of said parts or stations is conducted or established by means of an access code, said access code being available to an accessed part or station and requiring an identical access code to be provided to an accessing part or station at the time of conducting the transaction or establishing the connection, wherein said access code is one of a plurality of codes provided to said accessed part or station and available to said accessing part or station, said access code being selected from said plurality of codes at the time of conducting the transaction or establishing the connection such that no two transactions are conducted or no two connections are established with the same access code. Said system being programmed to avoid re-using such previously used codes, such that said code may be also be disabled or deleted to prevent it from being re-used, wherein a repetitive "multiple strikes" verification mechanism is used to ascertain a customer's electronic identity. Including a self-replenishment mechanism wherein access codes may be directly sent from the accessed station into the accessing station by means of an internet download, and thereafter, using said downloaded access codes in verifying said customer's identity when he seeks to conduct a secure transaction with the accessed station by means of a challenge-response mechanism. In one structural arrangement said accessed station comprising four distinct and interlinked modules may be interposed directly in between the accessing station and the protected resource 40 (Fig. 5). In an alternative arrangement, said verification module of accessed station may be integrated into the protected resource 16, 52 (Fig. 1 and 6).

Once an access code has been used to conduct a transaction or establish a connection between the two parts or stations it may be deleted from the system or otherwise disabled. This may avoid the risk that the access code will be reused by the system.

The plurality of access codes may be generated in any suitable manner and by any suitable means. The means for generating the access code preferably is capable of

generating non-repeating sequences of characters or numbers. In one form the plurality of codes may be generated via a pseudo random generator. In another form the plurality of codes may be generated via a custom designed software program. The basis for the software program should be randomness and free combination. In another form the software program may be a spreadsheet type program wherein a regular grid or pattern of characters or numbers can be mixed in a controlled manner to produce non-repeating sequences of characters and/ or numbers by means of such a manipulated combination mechanism. Such that each piece of access codes comprise numbers and characters of different denomination and digits.

The characters/ numbers may include Arabic numerals, Roman numerals, letters of the alphabet, morse codes, etc. in any order or combination. Preferably the access codes are generated independently of or external to the system such an approach may enhance security of the overall system by reducing risks associated with systems in which variable codes are generated internally.

The system of the present invention may include first code storage means associated with the accessing part of station of the system, such as an ATM terminal, personal computer, mobile telephone or the like. The first code storage means is adapted for storing one copy of the plurality of codes. The system may include second code storage means associated with the accessed part or station of the system, such as a bank or other service computer system or telephone exchange. The second code storage means is adapted for storing a second copy of the plurality of codes identical to the one copy stored in the first storage means. The first storage means may be incorporated into or with a transaction card such as an ATM card, a computer diskette, a smart card or integrated circuit microchip or the like. The first storage means may include a passive carrier such as a magnetic strip or the like or it may include an active carrier such as the integrated circuit microchip. Because a bank terminal system, computer service provider or telephone exchange typically will have a large number of users, the second storage means may be adapted to store a separate plurality of codes for each user. Each plurality of codes may be stored in the second storage means under a separate address. The address may be identified with a unique identity number

assigned to each respective user. The identity number may be that user's account number or it may be a different number associated with that user.

It is highly desirable that the last used code be removed or otherwise disabled from the second code storage means at least, as this will minimize the risk that the same code will be reused in a subsequent transaction. This task may be performed by the bank or other service computer system. The last used code may also be erased or otherwise disabled from the first code storage means. This latter task may be performed in any suitable manner and by any suitable means. In one form this may be carried out by application of heat or mechanical marking not unlike the manner in which a telephone card is disabled according to its level of use.

When a user with an ATM card having a particular identity number, say 9876, approaches an ATM terminal to make a transaction, the following sequence of events may take place:

(i) The bank computer system requests an unused code from the plurality of codes stored by the first code storage means, e.g. the ATM transaction card. The unused code will typically be the next unused code of the plurality of codes, but the plurality codes may be used in any predetermined sequence;

(ii) The bank computer requests the next unused code of the plurality of codes stored by the second code storage means under an address for the ATM card having identity number 9876;

(iii) Upon receipt of the respective codes from the first and second code storage means the bank computer compares the codes looking for a perfect match;

(iv) A perfect match between the two codes is interpreted as a successful verification of the identity of the user's transaction card, and card number 9876 is granted permission to proceed with the transaction;

(v) A mismatch between the two codes is interpreted as an unsuccessful verification of the identity of the user's transaction card and card number 9876 is denied permission to proceed with the transaction;

The present invention also provides a method of conducting a transaction or establishing a connection between at least two parts or stations by means of an access code, said access code being available to an accessed part or station at the time of conducting the transaction or establishing the connection and requiring an identical access code to be provided to an accessing part or station, said method including the steps of:

Making available a plurality of codes to said accessed and said accessing parts or stations;

Selecting, at the time of conducting the transaction or establishing the connection, one code from said plurality of codes; and

Using said selected code to conduct the transaction or establish the connection such that no two transactions are conducted or two connections are established with the same access code.

The access code system of the present invention may be used in place of an existing or conventional access code system or systems or it may be used in addition to an existing or conventional access code system or systems to upgrade the security of the latter. The improved system provided by the present invention may be incorporated into a newly designed code based access system or it may be provided by modifying an existing system to distinguish access codes according to the present invention from prior art codes they will hereinafter be referred to as "secondary" codes.

The system of the present invention may be used to enhance security of a door opening apparatus, in particular door opening apparatus which makes use of an electronic key for accessing secure areas such as safes, strong rooms, high security areas or the like. In the latter embodiment a set of secondary security codes according to the present invention may be loaded to a first code storage means associated with

the accessed part of the system. The accessed part may be a user inaccessible part of the door opening apparatus. The first code storage means may include an integrated circuit microchip, magnetic strip, smart card, computer diskette or the like. An identical set of codes may be made available to the accessing part of the system. The accessing part may be a user accessible part of the door opening apparatus. The accessing part may include an electronic key. The electronic key may include a second code storage means for storing an identical set of security codes. The second code storage means may include a magnetic strip, smart card, integrated circuit microchip, computer diskette or the like.

Brief Description of the Drawings

Preferred embodiments of the present invention will now be described with reference to the accompanying drawings wherein:-

Fig. 1 shows a diagramatic representation of one form of application of the present invention to bank terminals;

Figs. 2A, 2B and 2C show front, rear and cross-sectional views respectively of a dummy ATM card;

Figs. 3A, 3B and 3C show empty, loaded and cross-sectional views respectively of a carrier strip transfer apparatus;

Fig. 4 shows a cross-sectional views of an ATM card with carrier strip installed;

Fig. 5 shows a diagramatic representation of one form of application of the present invention to a mainframe computer system;

Fig. 6 shows a diagramatic representation of one form of application of the present invention to a mobile transceiver; and

Fig. 7 shows a diagramatic representation of one form of application of the present invention to a door opening apparatus.

Detailed Description of the Inventions

Referring to Fig. 1, there is shown an ATM access card 10 which serves as a carrier for secondary codes according to the present invention. In addition to the known magnetic strip (not shown) which carries the account number of the client, ATM card 10 includes a carrier strip 11 in which are stored secondary codes according to the present invention. Prior to using ATM card 10 at an ATM terminal 12, ATM card 10 is inserted into a dedicated disc drive of a Personal Computer (PC) 13. PC 13 is programmed to generate a non-repeating set of 100 secondary codes 14 and to write the set of codes 14 into carrier strip 11. An identical set of 100 codes is sent to data storage module 15 associated with the bank's main computer system 16. The set of codes 14 may optionally be sent to code replacement module 17 where they may be held temporarily pending transfer to storage module 15. After the set of codes have been written into carrier strip 11 and storage module 15 or code replacement module 17, PC 13 is programmed to delete the code set from its memory. This enhances security of the system by ensuring that no additional copies of the code set remain in existence.

ATM card 10 which carries identification serial number 9876 may then be inserted into a (modified) card slot associated with ATM terminal 12. The holder of ATM card 10 may key in his PIN number to commence a transaction and this may continue to provide a primary level of security as is known in the art. To provide a secondary level of security according to the present invention, main computer 16 sends a request A to ATM terminal 12 for the first unused code (ABCDEF) from the set 14 of 100 codes written into carrier strip 11 associated with ATM card 10. Main computer 16 also sends a request B for the first unused code from the identical set of 100 codes stored in data storage module 15 under an address for the ATM card carrying identification serial number 9876.

ATM terminal 12 sends reply C to computer 16 including the first unused code (ABCDEF) from carrier strip 11 and data storage module 15 sends reply D including the first unused code stored under the address corresponding to ATM card bearing serial number 9876. When computer 16 identifies a match between the codes included in replies C and D, it interprets this as a successful verification of the identity of ATM card

10 bearing serial number 9876 and grants permission E to ATM terminal 12 to proceed with the transaction.

When computer 16 identifies a mismatch between the codes included in replies C and D, it interprets this as an unsuccessful verification of the identity of ATM card 10 bearing serial number 9876 and denies permission to ATM terminal 12 to proceed with the transaction. A mismatch between the codes included in replies C and D indicates that an unauthorised penetration of the banking system may have taken place. Instead of barring further transactions in the event of a mismatch between the codes included in replies C and D, computer 16 may be programmed to request another code set each from ATM terminal 12 and data storage module 15. Preferably computer 16 is programmed to request three further code sets each from ATM terminal 12 and data storage module 15. If three consecutive code sets do not match, computer 16 may reasonably assume that the banking system has been penetrated by unauthorised elements and may bar further transactions of the account via the ATM card. Even if two out of three codes match computer 16 may still bar the transaction. Computer 16 may continue to request codes for verification until it has three consecutive matches, and may then return ATM card 10 to the user but not issue cash.

Computer 16 may advise the user via the screen associated with ATM terminal 12 to contact the local branch of his bank and seek assistance e.g. to have the account number and/ or code sets changed. The detected instance of potential breach of ATM card security may be recorded and communicated to the user immediately via telephone/ fax/ mail and/ or the next authorised transaction made by the user. Such that electronic messages serves to ensure secure electronic transactions.

When the holder of the ATM card commences a subsequent transaction, computer 16 sends a request to ATM terminal 12 for the second unused code (1234567). This process continues until all 100 secondary codes have been used up one at a time. When all 100 codes sets have been used up the user will be advised via ATM terminal 12 to contact his bank to have the defunct carrier strip 11 replenished with a fresh set of 100 codes. Carrier strip 11 may be replenished by rewriting. Alternatively,

if the technique used for disabling/deleting used codes has harmed the integrity of the carrier strip 11, carrier strip 11 may be removed from the ATM card and replaced with a fresh carrier strip. The fresh carrier strip may be supplied to the bank branch from a central location already written with a new set of 100 codes. The fresh carrier strip may be supplied attached to a blank or dummy card to facilitate handling, programming and transfer of the carrier strip to a customer's ATM card.

Referring to Figs. 2A-C there is shown a dummy card 20 formed from 0.4mm thick plastics. This is about half the thickness of an ATM card. Fresh carrier strip 21 is attached to the front of dummy card 20 via a layer of adhesive 22. As shown in Fig. 2B, dummy card 20 is perforated at edges 23 adjacent the perimeter of carrier strip 21 and carrier strip 21 is arranged to break away from the main body of dummy card 20. A local layer of adhesive 24 overlaying carrier strip 21 is applied to the back of dummy card 20 as shown in Figs. 2B and 2C. Adhesive layer 24 is protected by a removable non-stick plastic cover 25.

Fresh carrier strip 21 may be transferred to a customer's existing ATM card via an apparatus as shown in Figs. 3A to 3C. Referring to Fig. 3A, the apparatus includes hinged upper and lower panels 26, 27. Upper panel 26 includes a recess 28 for receiving an ATM card. The ATM card includes a recess 10A for receiving carrier strip 21 (refer Fig 4.) Lower panel 27 includes a recess 29 for receiving the dummy card 20. Lower panel 27 also includes an embossing bar 30 positioned so that it coincides with carrier strip 21 when dummy card 20 is received in recess 29.

Embossing bar 30 is positioned so that it also coincides with recess 10A in the ATM card when the latter is received in recess 28 and upper and lower panels 26 and 27 are closed against each other. Referring to Fig. 3B, embossing bar 30 in its rest position is below the level of the non-recessed face of lower panel 27 by the thickness of dummy card 20. Embossing bar 30 rests on see-saw brackets 31, 32. See-saw brackets 31, 32 are mounted for pivotal movement about respective pivot points 33, 34. The inner ends 35, 36 of brackets 31, 32 abut embossing bar 30. The outer ends 37, 38 of brackets 31, 32 project beyond the face of lower panel 27 such that when upper and

lower panels 26 and 27 are closed against each other, brackets 31, 32 pivot, lifting embossing bar 30 approximately 0.5 mm above its rest position.

In operation an ATM card 10 devoid of its carrier strip is received in recess 28 and dummy card 20 with carrier strip 21 intact is received in recess 29 as shown in Fig. 3C. To effect transfer of carrier strip 21 from dummy card 20 to ATM card 10, cover 25 is peeled away from adhesive layer 24 and upper panel 26 is closed firmly against lower panel 27 of the apparatus. This caused embossing bar 29 to lift to a position about level with the non-recessed face of panel 27, breaking perforated edges 23 and causing carrier strip 21 to lodge into recess 10A in ATM card 10 (refer Fig. 4). Upon opening of the apparatus, transfer of carrier strip 21 from dummy card 20 to the customer's ATM card 10 should be complete.

Transfer of carrier strip 21 from dummy card 20 to the customers ATM card 10 may also be performed manually. This may be done by firstly removing the cover 25 from adhesive layer 24 and placing dummy card 20 on top of ATM card 10, both in an upright and face up position. The two cards may be held firmly together e.g. by means of adhesive tape applied to the tops and sides of the cards. The two cards should then be placed on a hard surface such as the edge of a table and an embossing bar approximately equal in dimensions to carrier strip 21 (78 mm x 4 mm) placed on the top of carrier strip 21. The embossing bar should then be pressed down firmly with both thumbs. The thumbs may be slid along the length of the embossing bar until carrier strip 21 breaks away from dummy card 20 along its perforated edges 23 and is pushed into recess 10A in ATM card 10. The adhesive tapes may then be removed and transfer of carrier strip 21 to ATM card 10 should be complete.

Each bank branch may hold a large number of dummy cards with attached replacement carrier strips. To maintain security of the allocation process the customer may select at random a replacement carrier strip from a batch of say 1000 replacement strips. When the customer selects his carrier strip it is affixed to his ATM card and the central bank computer is notified of the choice. The central bank computer then

associates its second copy of the set of codes identical to the chosen replacement strip with the customer's account or other identification number.

The system shown in Fig. 5 protects a mainframe computer system 40 from hacking by way of external links to the computer system 40. Security is typically provided in this context by way of a common password for all authorised users of computer system 40 and optionally another password for individual users. The passwords are usually changed once a week. This allows a hacker who gains access to the password or passwords to commit repeated break-ins over the period of currency of the password(s) and to gain access to confidential information and corrupt the system with unauthorised data or a virus.

The present invention allows operators of computer systems to substantially limit risk of random break-ins and to avoid repeated break-in activities.

Referring to Fig 5 there is shown a personal computer (PC) 41 connected to computer system 40 via connection 42 such as the internet, and a verification module 43. The accessed station comprising modules 43, 45, 46 and 47 is interposed directly in between the accessing station 41 and protected resource 40. Module 45 serves as a codes generator, while module 43 performs the main verification tasks by means of a "challenge-response" mechanism. Module 46 is configured to store all the access codes deployed for use by the system, while module 47 serves as a transit warehousing facility for storing fresh groups of codes 14 temporarily prior to assignment. The modules are configured to perform specialized verification tasks with great efficiency in order to accommodate high load demands by customers as a service provider's computer typically have a large number of users. Before access to computer system 40 can be granted verification module 43 must receive a valid code(s) from PC 41. The valid code(s) may include the usual password or passwords and includes a secondary code according to the present invention. A set of secondary codes 44a may be stored on an authorisation diskette 44 which serves as a carrier for the secondary codes. Diskette 44 is adapted to store 100 sets of secondary codes. The set of secondary

codes 44a is loaded to diskette 44 via PC 45 belonging to or being under the control of the owner or operator of computer system 40.

Once it is loaded with the secondary codes 44a diskette 44 is supplied via a secure route to the authorised user of computer system 40. The authorised user is obliged to store diskette 44 in a secure and preferably locked or otherwise restricted location. Diskette 44 will typically be available for use with a designated PC/ terminal i.e. a terminal having a specific E-mail address, unless a roaming authority has been granted.

Diskette 44 should only need to be sent to new clients or first time users (including replacements for lost, barred and malfunctioning disks) because subsequent replacements codes (i.e. after a current set of 100 codes has been used up) can be sent to the user's PC 41 via connection 42 after it has been verified. A set of 100 secondary codes identical to the set loaded to diskette 44 is sent from PC 45 to storage module 46 associated with verification module 43. The set of codes may optionally be sent to code replacement module 47 where they may be held temporarily pending transfer to storage module 46.

When a user requests access to computer system 40 and (optionally) keys in his passwords into PC41, verification module 43 sends a requests (challenge) to PC41 via connection 42 for the first unused code from the list of 100 codes stored on diskette 44. Module 43 also sends a request A (challenge) for the first unused code from the identical set of 100 codes stored in storage module 46 under an address specific to PC41. PC41 sends a reply (response) to verification module 43 including the first unused code stored on diskette 44, and storage module 46 sends reply B (response) to verification module 43 including the first unused code stored under the address which corresponds to PC41. When verification module 43 identifies a match between the codes received from PC41 and storage module 46 it interprets this as a successful verification of the identity of PC41 and grants access to PC41 to connect to computer system 40.

Even if the first set of codes is not immediately deleted after use for any reason, the verification software should be programmed so that it avoids reusing a previously used code. When the user next requests access to computer system 40, verification module 43 sends a request for the second unused code. This process continues until all 100 secondary codes have been used up one at a time. Diskette 44 will then be defunct as it has no more verification codes available and must be replenished or replaced.

In one form a code replacement program may be activated upon positive verification of an access using the last or 100th code. Upon detecting a verification which utilises the 100th code, code replacement module 47 is activated to choose at random a new group of 100 secondary codes stored in module 47 and to download this to diskette 44 via line 48, module 43, line 42 and PC41. During this process an image appears on the screen of PC41 warning the user not to remove diskette 44 from PC41. Module 47 also loads an identical set of codes to storage module 46. The verification software may then assign via line 49 the identity of PC41, such as its E-mail address, to the set of codes just loaded to storage module 46. Code replacement module 47 may hold a large stock of unused code sets (e.g. 1000) ready to be downloaded upon receiving a request from verification module 43.

When verification module 43 identifies a mismatch between the codes received from PC41 and module 46 it interprets this as an unsuccessful verification of the identity of PC41 and denies further access to PC41 to connect to computer system 40. A mismatch between the codes received from PC41 and module 46 indicates that an unauthorised penetration of the computer system may have taken place. The user is advised of this status and of the need for increased security/access to PC41 to prevent further unauthorised activities and/or the need to change passwords, diskette 44 etc.

Instead of barring further access in the event of a mismatch between the codes, module 43 may be programmed to request another code set each from PC41 and data storage module 46. Preferably module 43 is programmed to request a further three code sets each from PC41 and data storage module 46. If three consecutive code sets do not match, module 43 may reasonably assume that the computer system has been

penetrated by unauthorised elements and may bar further access to PC41. Even if two out of three codes match module 43 may still bar access. Module 43 may continue to request codes for verification until it has three consecutive matches, and only then may grant access to PC41.

The system shown in Fig. 6 protects a mobile transceiver such as a cellular telephone from unauthorised use. Security is typically provided in this context by means of an electronic serial number (ESN) which establishes the identity and authenticity of an incoming call placed through a host transceiver. During the process of registration and activation of a new cellular telephone, matching sets of ESNs are respectively placed in the mobile transceiver and in the data bank of a main telephone exchange.

When a call is placed through the mobile transceiver, the transceiver transmits its ESN followed by the telephone number of a recipient transceiver. The transmitted signal is relayed via a receiving dish to the data bank of the telephone exchange. The ESN of the mobile transceiver is then compared to the matching ESN in the databank. When a match is established, the call is recognised by the telephone exchange as genuine and is authorised passage to the next stage (where no match is established between the transceiver ESN and the data bank ESN, the call is rejected and refused passage through the main exchange). The telephone number of the recipient transceiver is then sent by the telephone exchange to a transmitting tower for transmission to the recipient transceiver.

Referring to Fig. 6, there is shown a host transceiver 50 linked to a recipient transceiver 51 (not shown) via telephone exchange 52 and respective transceiver stations 53, 54. Before access to recipient transceiver 51 can be granted, telephone exchange 52 must receive a valid code(s) from host transceiver 50. The valid code(s) may include a conventional ESN and includes a secondary code according to the present invention. A set of secondary codes may be stored in an integrated circuit microchip/ smart card (IC) 55 fitted to host transceiver 50.

IC 55 is in addition to the usual ESN integrated circuit microchip/smart card 56 fitted to host transceiver 50. IC 55 is adapted to store 500 sets of secondary codes 55a.

The set of secondary codes 55a is transferred to IC 55 via PC 57 belonging to or being under control of the owner or operator of telephone exchange 52. PC 57 includes a dedicated IC writer for this purpose. Once IC 55 is programmed, it is sent to a local branch office of the telephone service operator or his agent for installation to a new subscriber's transceiver or for replacement of a defunct IC i.e. an IC which has exhausted all of its secondary codes.

A set of 500 secondary codes identical to the set 55a stored in IC 55 is sent from PC57 to storage module 58 associated with telephone exchange 52. The set of codes may optionally be sent to code replacement module 59 where they may be held temporarily pending transfer to storage module 58.

When host transceiver 50 places an outgoing call it transmits its ESN which is picked up by transceiver station 53 and relayed to telephone exchange 52. The transmitted ESN is then compared to the matching ESN in the data bank of telephone exchange 52. When a match is established the ESN is recognised by telephone exchange 52 as legitimate and the call is authorised passage to the next stage.

According to the present invention telephone exchange 52 sends a request A to host transceiver 50 via transceiver station 53 for the first unused code from the set of 500 codes 55a stored in IC 55. Telephone exchange 52 also sends a request B for the first unused code from the identical set of 500 codes stored in storage module 58 under an address specific to host transceiver 50. In practice the storage address may be associated with the unique ESN assigned to host transceiver 50.

Host transceiver 50 sends a reply C including the first unused code stored in IC 55 to telephone exchange 52 and storage module 58 sends reply D to telephone exchange 52 including the first unused code stored under the address which corresponds to host transceiver 50. When telephone exchange 52, identifies a match between the codes included in replies C and D, it interprets this as a successful verification of the host transceiver 50 and allows the telephone number of the recipient transceiver 51 sent by host transceiver 50, to be transmitted to transceiver station 54 and relayed to recipient transceiver 51.

Even if the first set of codes is not immediately deleted after use for any reason, the verification software should be programmed so that it avoids reusing a previously used code. When the subscriber next places an outgoing call, telephone exchange 52 sends a request for the second unused code. This process continues until all 500 secondary codes have been used up one at a time. IC55 will then be defunct as it has no more verification codes available and must be replenished/ replaced.

When all 500 codes have been used up (in practice this may be a lesser number to allow some reserve calls to be made before receiving a replacement for IC55) the telephone exchange can advise the subscriber (e.g. by means of a recorded message following verification of, say, the 490th call) to contact his local branch to have the defunct (or soon to be defunct) IC 55 replaced with a fresh IC. The fresh IC may be supplied to the branch office already loaded with a new set of 500 codes. Each branch office may hold a large number of replacement IC's to maintain security of the allocation process the subscriber may select at random a replacement IC from a batch of, say, a 1000 replacement ICs. When the subscriber selects his/ her IC it may be fitted to his transceiver and the telephone exchange notified of the choice. The telephone exchange may then associate its second copy of the set of codes identical to the chosen replacement IC with the subscribers ESN or other identification number.

IC 55 may be located in an easily accessible position in the associated transceiver to enable replacement of defunct ICs. In some embodiments IC 55 may comprise a smart card. IC 55 also may be integrated with ESN IC 56. Typically a transceiver will require modification to accommodate IC55. This may be done by way of a sliding carrier not unlike a smart card. New transceivers may be constructed with a built-in slot for receiving IC 55 and/ or associated carrier.

Referring to Fig. 7, there is shown a safe/ strong room 60. Safe/ strong room 60 includes a code based door opening apparatus according to the present invention.

The door opening apparatus includes a first code storage means associated with a user inaccessible part of the door opening apparatus. The first code storage means is adapted for storing a set of secondary codes 61. The first code storage means include a

computer diskette 62. The diskette 62 may be adapted to store 100 sets of secondary codes. The set of secondary codes 62 is loaded to diskette 62 via PC 63.

Once it is loaded with secondary codes 61 diskette 62 is installed to the user inaccessible part of the door opening apparatus.

PC 63 is used to load an identical set of secondary codes 61 to a second diskette 64. Diskette 64 is in possession of the owner of safe/ strong room 60 or other authorised person, who is obliged to store diskette 64 in a secure and preferably locked or otherwise restricted location. When the owner/ authorised person requires access to safe/ strong room 60, diskette 64 serves as an electronic key to activate the door opening apparatus and gain access to safe/ strong room 60.

When diskette 64 is inserted into the user accessible part of the door opening apparatus associated with safe/ strong room 60, the door opening apparatus requests the first unused code from the list of 100 codes stored on diskette 62. The door opening apparatus also requests the first unused code from the identical set of 100 codes stored in diskette 64. When the door opening apparatus identifies a match between the codes received from diskette 62 and diskette 64 it interprets this as a successful verification of the identity of the electronic key and opens the door.

Finally, it is to be understood that various alterations, modifications and/ or additions may be introduced into the constructions and arrangements of parts previously described without departing from the spirit or scope of the invention.

CLAIMS:

1. A method of verification characterized in that the computer verification software (43) is programmed to avoid re-using previously used access codes (14) for conducting further transactions or for establishing further connections; such that no two transactions are conducted or no two connections are established with the same access code.

2. A system as recited in Claim 1 including the steps of :

providing a computerized software running in the verification module (16, 43, 52) programmed to avoid re-using previously used access codes; said

software being programmed to select at random, access codes for conducting verifications in "real-time"; wherein said computer software can be used to selectively,

avoid re-using said previously used "spent" codes for conducting further transactions or for establishing further connections; wherein said access codes are only used once.

3. A system as recited in Claim 1 wherein said previously used codes (14) are disabled to prevent them from being re-used.

4. A system as recited in Claim 1 wherein said previously used codes (14) are deleted to prevent them from being re-used.

5. A method as recited in Claim 1 wherein verification access codes (14) and messages sent directly between service providers and their subscribers are used in establishing secure electronic connections for conducting secure electronic transactions.

6. A system as recited in Claim 5 wherein said system is characterized in that electronic security messages and access codes (14) sent between operators of computer systems (16, 43, 52) and their customer's wireless transceiver (50) are directly used in the course of conducting a secure electronic cash or monetary transaction; wherein,

said information, advisories, instructions, confirmation, rejection, reminders, verification and authentication data contained in said messages are used in securing electronic payment transactions; said improvement comprising of

sending and delivering said messages and access codes by means of electronic communication systems such as Internet connection (42).

7. A system as recited in Claim 5 wherein the electronic communication system such as the internet connection (42) is used as a means of replenishment for sending, delivering and distributing groups of access codes (14) and verification messages from said service provider's computer system into the subscriber's electronic communication access device (50); wherein,

when said subscriber seeks to establish a connection to conduct a secure transaction with protected resource computer (40),

verification module (43) requests and challenges subscriber's electronic device (50) to provide valid access codes (14); wherein,

said access codes are directly sent from said subscriber's personal gadget (50) to the service provider's verification module (43) and used to establish the identity of said subscriber; wherein,

said access codes are used up one piece at a time to secure financial and monetary transactions until the storage memory means are exhausted such that upon activation of the 490th piece of access codes,

module (43) initiates a self-replenishment program to download a fresh group of 500 pieces of access codes (14) into mobile transceiver (50).

8. A method of verification characterized by an automated repetitive "multiple strikes" verification capability comprising:

a verification software module (43) capable of automatically activating and launching a series of verifications repeatedly;

for a triple strike of at least three pieces of access codes (14) repeatedly and consecutively until three successively, successful verifications have been obtained in order to establish a secure connection, or to conduct a secure transaction.

9. A ~~system~~ as recited in Claim 8 wherein said repetitive "multiple strikes" verifications sequence is initiated by a triggering event, said triggering event being the failure of an initial verification sequence.

10. A method as recited in Claim 8, characterized by using a repetitive "multiple strikes" verification sequence for authenticating customers; said improvement including the steps of,

providing a software program running on a computer wherein, computer (16) automatically initiated said "multiple strikes" verification sequence; means wherein, said

computer (16) requested another access code (14) each from the smartcard storage means (55) mounted on ATM transaction card (10) in ATM terminal (12); and the storage module (15),

said computer being preferably programmed to request a further three access codes each from ATM terminal (12) and data storage module (15) for verification.

11. A system as recited in Claim 10, wherein said repetitive multiple strikes verification sequence is used in controlling access between a personal computer (41) and Service Operator's accessed station comprising verification modules (43, 45, 46, 47); before access to mainframe computer system (40) can be granted.

12. A system as recited in Claim 10, wherein said repetitive multiple strikes verification sequence is used in controlling access between mobile transceiver (50) and telecommunication operator's computerized main exchange (52) and verification modules (57, 58, 59).

13. A system as recited in Claim 8, characterized by an automatic self- replenishment process wherein, defunct storage memory means (11, 44, 55) which has been depleted and exhausted of valid access codes (14) are automatically replenished with new supplies of access codes; said self-replenishment process being automatically initiated by the verification software program (43) ensuring a continuous supply of fresh access codes for verification; said improvement comprising of the steps of,

maintaining a stockpile of fresh groups of new access codes (14) in module (47) in support of said automated self-replenishment mechanism; means of,

providing a trigger mechanism initiated by a low number of fresh access codes remaining in the storage memory devices (11, 44, 55);

providing a self-replenishment mechanism enabled by means of an Internet download (42) implemented by said software program, said download being automatically activated; wherein, "spent" access codes (14) that have been previously used, are replaced, rewritten, "updated" and "topped up" with fresh access codes;

providing an auto-select mechanism wherein, one fresh group of new access codes (14) is randomly selected out of a stockpiled reserve of 1,000 groups, for conveyance via electronic communications systems such as the Internet connection (42); directly

sending said group 14 into the end-user's utility appliances such as mobile transceivers (50), Automated Teller Machine terminals (12), personal computers (41); and

associated storage means and memory devices such as ATM cards (10), smartcards (55), integrate circuit microchips (55), magnetic strips (11) and computer diskettes (44, 62, 64).

14. A system as recited in Claim 13, further characterized by a self-replenishment mechanism and means wherein, a duplicate copy of the plurality of access codes (14), is concurrently assigned, and auto-loaded from the code replacement module (17, 47, 59) into the storage module (15, 46, 58) of the service provider's accessed station under an address which corresponds to the storage means (11, 44, 55) of the accessing station (12, 41, 50) such as the unique identity assigned to each respective user.

15. A system as recited in Claim 13, wherein, performing verifications until ten pieces of valid access codes remains in the memory means; said improvement comprising of,

providing a means wherein, a verification process utilizing said 490th access code serves to act as the trigger mechanism, prompting the service provider's verification software running in module (43) to initiate an auto-selection and thereafter an Internet download sequence;

after said user has been verified; providing means of

selecting a fresh group (14) comprising 500 pieces of access codes and downloading said fresh group directly into said user's electronic communication access device (12, 41, 50) and storage memory means (11, 44, 55).

16. A system as recited in Claim 13, wherein said improvement comprises an auto-selection mechanism is initiated for choosing at random, one specific group of new access codes (14) out of the reserved 1,000 groups of access codes stockpiled in module (17, 47, 59) for auto-loading.

17. A system as recited in Claim 13, further comprising means of a self-replenishment mechanism of the software program which is activated after the user has been verified; wherein

said group of access codes (14) is sent by means of an Internet download (42) into the user's electronic communication access device and storage means; wherein

said means of conveying being wire-line electronic communication systems (ATM terminal 12).

18. A system as recited in Claim 17, wherein said means of downloading comprises wireless electronic communication systems into mobile transceiver (50).

19. A system as recited in Claim 18, wherein said download by electronic communication systems comprises the Internet connection (42) into personal computer (41).

20. A system as recited in Claim 19, further comprising the means for storing said access codes (14) from said user's electronic communication access devices into related receiving, or storage-memory means such as diskettes (44), magnetic strips (11) and ATM Cards (10), directly associated with said Automated Teller Machine terminals

(12), mobile hand-phones (50) and personal computers (41).

21. A system as recited in Claim 20, wherein said storage-memory means comprises smart-cards (55).

22. A system as recited in Claim 21, wherein said storage-memory means comprises integrated circuit microchips (55).

23. A method of conducting secure transactions characterized by means of electronic messages and verification access codes (14) wherein, said messages and access codes are used in securing electronic transactions between service providers and subscribers.

24. A method as recited in Claim 23 wherein, said improvement comprises the use of electronic security messages and access codes (14) in verifying said customer's electronic identity for establishing secure electronic connections.

25. A method as recited in Claim 23 wherein, said improvement comprises the use of electronic security and verification messages in securing electronic transactions; said messages sent between said service providers and end-users being used for conveying;

user authorization, authentication and verification related needs; need for replenishment of new codes (14) into defunct or soon to be defunct I.C. microchips or smart cards (55); replacement of said defunct or soon to be defunct I.C. microchips or smart cards; potential and attempted security breaches and warnings; are instantly,

transmitted between the accessed station (service provider's main telephone exchange 52) and the accessing station (subscriber's electronic communication access devices) comprising mobile transceiver (50); wherein,

said customer can be immediately notified of the detected instance of security breaches such as unauthorized penetration of the computer system; and

preventive measures and risks mitigating actions to be taken by said user such as increased security and access to PC41, change of passwords, storage means, account numbers or access codes; thereby securing electronic monetary transactions and connections.

26. A method as recited in Claim 23, wherein operators of computer systems utilizes electronic communications system such as transceiver stations (53, 54) and the internet (42);

to download access codes (14) and security messages pertaining to the usage of said access codes; said improvements comprising, the

use of said access codes and security messages in conducting secure electronic business transactions; and

in establishing secure electronic connections for the purpose of commerce; said

transmission being carried out between said service operator's computerized telephone exchange (52) and subscriber's electronic transceiver (50) via said wireless transmitting towers (53, 54) and receiving dish.

27. A method as recited in Claim 26, wherein said accessing station or subscriber's electronic communication access device comprises personal computer (41).

28. A method as recited in Claim 27, wherein said accessing station or subscriber's electronic communication access means comprises part of a bank terminal system, ATM terminal (12).

29. A method as recited in Claim 23, including means of conveyance wherein said security messages in the form of data, voice and visual image (graphics) based security related information and access codes (14) from the service provider is delivered directly into its customer's personal electronic gadgets or accessing station (12, 41, 50); said improvement comprising of,

providing a means wherein said users upon receiving said messages acts accordingly on said information received to resolve verification related needs as directed by the service provider in preventing and mitigating electronic frauds;

allowing operator of computer system (40) to substantially limit risk of random break-ins by a computer hacker, and to avoid repeated break-ins of said system (40);

preventing said hacker from stealing confidential information from said computer system (40), or corrupting it with unauthorized data or a virus; such as to

change passwords, change ESN, change PINs, change access codes, change access codes storage means (45); or to

contact the local branch office of said service provider to seek assistance and resolve security and access codes verification related needs;

for the purpose of conducting secure transactions and establishing secure connections.

30. A method as recited in Claim 23, wherein electronic messages sent between service providers and their subscribers are used in conducting secure electronic transactions and in establishing secure electronic connections; wherein, said

messages are sent, delivered and received between said telecommunication service operator's exchange (52) and

said subscriber's electronic communication access device such as a mobile transceiver (50), for the purpose of securing business and commercial transactions.

31. An access control system characterized by a structural configuration wherein the service provider's accessed station or verification computer system comprises four individually distinct components; said improvement including providing means of an,

independent spreadsheet access codes generator module (13, 45, 57); an

access codes verification module (16, 43, 52); an

access codes storage module (15, 46, 58); and an

access codes replacement module (17, 47, 59); in a structural arrangement wherein said 4 components comprising said accessed station are inter-linked with each other,

providing a means of tasks specialization, wherein each individual component of the access control system is configured to perform specific access codes verification tasks with great efficiency to complement each other's needs in handling the high volume processing demands of the accessing stations (12, 41, 50); wherein

said system workload can be extremely high as a bank terminal system, computer service provider or telephone exchange typically have a large number of users.

32. A method as recited in Claim 31, said improvement further comprising of a structural arrangement wherein said accessed station's verification computer system comprises of the;

access codes verification module (43); access codes generation module (45); access codes storage module (46); access codes replacement module (47); being,

interposed directly in between said accessing station (41) and the protected resource, mainframe computer system (40), controlling all access into and out of said computer (40).

33. A method as recited in Claim 31, said improvement further comprising of a structural arrangement wherein the software for said access codes verification module is incorporated into the bank computer system; means wherein,

said integrated access codes verification module and bank computer system (16) being supported by said specialized individual modules comprizing;

access codes generator module (13); access codes storage module (15); access codes replacement module (17); and

forms the accessed station together with these three components; in conducting secure transactions by customers via accessing stations comprising ATM terminal (12).

34. A method as recited in Claim 33, wherein the software for said access codes verification module is incorporated into the telephone exchange;

providing a means wherein, said integrated access codes verification module and telephone exchange (52) is supported by said specialized individual modules

comprizing;

access codes generator module (57); access codes storage module (58); access codes replacement module (59); and

forms the accessed station together with these three components; in establishing secure connections by subscribers via accessing stations comprising cellular telephone (50).

35. A system as recited in Claim 31, wherein the independent stand-alone spreadsheet access codes generator module (13, 45, 57) specializes in generating access codes (14) used for verification; said improvements comprising,

providing means wherein, said independent generator is physically segregated from the other components, but can be connected to the other three components of said system when required,

to transfer and download new groups of access codes (14) into storage means (11, 44, 55) associated with the accessing stations (12, 41, 50); and the codes storage module (15, 46, 58); or,

alternatively into the access codes replacement module (17, 47, 59) where it is stockpiled, pending deployment.

36. A system as recited in Claim 31, wherein the access codes storage module (15, 46, 58) serves as a specialized storage means and stores all of the accessed station's plurality of access codes (14) for each individual subscriber of said service provider in its databank; said improvement including the steps of,

providing a computerized storage module (15, 46, 58) which serves as a "ware housing" facility, wherein said module is adapted to store a separate plurality of codes for each subscriber such that each group (14) comprises 100 pieces or

500 pieces of access codes per group;

providing an administrative means for the authorization and authentication of subscribers, wherein each said plurality of codes can be stored under a separate address, wherein said address can be identified with a unique identity number assigned to each respective subscriber by said service provider; wherein,

said identity number can be said subscriber's account number or a different number associated with said subscriber's unique identification number, unique ESN, email, account number associated with said subscriber.

37. A method as recited in Claim 31, said improvement including means wherein the access codes verification module (16, 43, 52) specializes in processing access codes verification and performs the main verification tasks of said computerized access control system.

38. A method of an automated self-replenishment mechanism characterized in that the access codes replacement module (17, 47, 59) specializes in providing a temporary storage means for stockpiling new or fresh groups of access codes (14) prior to assignment, download and allocation into individual subscriber's accounts; including the steps of,

providing a transit point or facility for storing a large stockpile comprising thousands of groups of new and fresh codes on standby, ready to be downloaded upon requisition from the access codes verification software module (16, 43, 52);

providing a trigger mechanism wherein, upon detecting a verification utilizing the last, or 100th code, verification module (43) activates module (47) to choose at random a new group of 100 access codes stored in module (47);

providing a means of delivering and downloading this group of codes to storage means (44) via line (48), module (43), line (42) and accessing station (PC 41); wherein,

replacement module (47) also loads an identical copy of access codes into storage module (46) simultaneously; wherein,

verification module (43) may then assign via line (49) the identity of PC 41 such as its E-mail address to the group of codes just loaded into storage module (46).

39. A method as recited in Claim 38, wherein said access codes replacement module (17, 47, 59) holds a large stock of new groups of access codes (14); said improvement including means of,

providing said computerized replenishment module (47) which serves as a "transit ware-housing" facility wherein, said module kept in reserve an inventory of software goods and products such as access codes (14) prior to distributing said merchandize; wherein, said

stock-pile comprise thousands of groups of new access codes (14); wherein, each said

group (14) comprises 500 pieces of fresh access codes; each individual piece of access code being different from the other;

providing a means for sending said groups of codes (14) from modules (17, 47, 59) into the customer's computerized electronic communication stations (12, 41, 50);

by means of electronic communications system and the Internet connection (42).

40. A system as recited in Claim 38, wherein said specialized module (47) which serves as a "transit ware-housing" facility for stock piling an inventory of software goods and products such as access codes prior to sending, conveying, delivering or distributing said merchandize directly from the service provider's computer into the subscriber's electronic personal gadgets (41) and (50) by means of electronic communications system such as the Internet connection (42).

41. A method characterized in that the access codes verification software module (43) specializes in processing verifications of the accessing stations (41) before a secure access can be granted into the protected resource, mainframe computer (40) in order to conduct a secure transaction or to establish a secure connection; said improvement including the steps and means of;

making available a plurality of codes to said accessing station (41); wherein said access codes (14) is sent by means of an Internet download from said accessed station (43) into said accessing station (41); wherein,

upon detecting a verification using the last (100^{th}) code, said verification software program initiated a randomized selection of and thereafter, the download of a new group of access codes (14) to replenish a defunct, or soon to be defunct storage means (11, 44, 55) via Internet connection (42);

providing a selection mechanism wherein module (43) is programmed for randomly selecting one valid access code (out of 100 codes) from the plurality of codes (14) for verification right at the time of conducting said transaction or establishing said connection;

using said randomly selected access code in "real-time" for conducting said transaction or establishing said connection;

providing a "challenge-response" mechanism wherein, verification module (43)

requests (challenge) accessing station (41) to provide this selected code, such that responsive to said requisition, (41) and (46) retrieves and sent said selected code in reply (response),

receiving the reply from (41), and verifying said access code (response) received from (41), against a plurality of said selected code (response) received from module (46); wherein,

a perfect match means a positive verification of (41); such that,

no two transactions are conducted or no two connections are established with the same access code;

preventing further use of said (by now "in-valid") previously used code by means of said software verification module (43) being programmed to avoid re-using such previously used codes (14) for conducting further verifications;

providing a "multiple-strikes" authentication mechanism, wherein upon failure of an initial verification attempt, said software (43) initiates a repetitive verification sequence in which a minimum of at least three positive verifications are required to establish the identity and authenticity of said accessing station (41);

providing a "barring mechanism" wherein said verification failure rendering said customer being denied permission to proceed with carrying out a transaction or connection; wherein,

said verification failure also renders said account being barred from carrying out further electronic transactions or establishing further electronic connections;

providing a messageing mechanism, wherein said software module is programmed for sending verification messages into said accessing station (41) to

advise users of verification status and security breaches.

42. A system as recited in Claim 41, said improvement comprising a replenishment mechanism wherein said verification module software (43) initiated an Internet download via connection (42) of new and fresh access codes (14);

providing a triggering mechanism wherein, upon detecting a verification using the last, or 100th code, verification module (43) activates code replacement module] (47); to

choose at random a new group of 100 access codes stored in module (47); and to

download this group (14) into storage means (44) via line (48), module (43), line (42) and PC (41).

43. A method as recited in Claim 42, said improvement comprises providing means wherein said access codes verification module (43) automatically activates,

replacement module (47) to load an identical group of codes to storage module (46); wherein,

verification software of module (43) then assigns via line (49) the identity of personal computer (41) such as its E-mail address, to the group of codes just loaded into storage module (46).

44. A system as recited in Claim 42, said improvement comprising means wherein said internet download is carried out upon detection of a secure verification using the 490th code (out of a group comprising 500 access codes) by the verification module software; wherein, said group downloaded contains 500 pieces of access codes.

45. A "challenge-response" system as recited in Claim 41, wherein verification module (43) requests (challenge) accessing station (41) and the codes storage module (46) to provide a selected code; said improvement comprising means wherein, responsive to such a request;

accessing station (41) obtains said selected code from its storage means and sent said code in reply (response) to module (43); wherein at the same time,

codes storage module (46) retrieves said selected code stored in its memory means and sent said code in reply (response) to module (43); means wherein,

verification module (43) upon receiving said replies; verified said code received from accessing station (41) against a plurality of said code received from module (46); wherein,

a perfect match means a successful verification of the identity of accessing station (41).

46. A system wherein a spreadsheet type program generator (13, 45, 57, 63) is used to generate a plurality of access codes (14) for verification, wherein said system is characterized in that said spreadsheet is used to mix a regular grid or pattern of characters and numbers in a controlled manner to produce non-repeating sequence of characters and numbers.

47. A system as recited in Claim 46, wherein said independent access codes generator (13, 45, 57, 63) and spreadsheet software means is externally located from the accessing and accessed stations.

48. A system according to Claim 47, wherein said verification system (16, 43, 52) is programmed to disable previously used codes after they have been used for verification; said improvement comprising means wherein, said

system is programmed to avoid re-using previously used codes for verifications; such that, even if a similar replica or copy of a previously used code (14) happens to be recycled or re-submitted for use; said software is programmed to avoid reusing them; said

system is programmed to selectively avoid using said disabled codes; said

said system is programmed to prevent further use of a previously used code to avoid selecting such disabled previously used codes for verification, for establishing a secure connection or for conducting a secure transaction.

49. A system according to Claim 46, wherein said plurality of access codes (14) is generated by means of a spreadsheet type generator (13, 45, 57, 63) arranged to produce non-repeating sequence of codes; said improvement includes providing means of a "manipulated-combination" mechanism wherein,

a regular grid or pattern of characters and numbers are mixed in a controlled manner to produce non-repeating sequence of characters and numbers.

50. A system according to Claim 49, wherein each code (14) includes a sequence of "alphanumeric" characters and numbers comprising Arabic numerals, Roman numerals, letters of the alphabets, and morse codes.

51. A system according to Claim 46, wherein the plurality of access codes (14) is generated external to the accessed (16, 40, 52) and accessing stations (12, 41, 50).

52. A system according to Claim 46, said improvement comprises means wherein, said plurality of access codes (14) is at least 500 pieces.

53. A system according to Claim 46, said improvement including storage means

associated with said accessing station (12, 41, 50) for storing one copy of said plurality of codes (14).

54. A system according to Claim 46, said improvement including storage means associated with said accessed station (16, 43, 52) for storing a duplicate copy of said plurality of codes identical to said one copy stored in said storage means of the accessing station (12, 41, 50).

55. A system according to Claim 54, wherein said improvement comprises storage means associated with the accessing station (12, 41, 50) including one of an ATM transaction card (11), a smart card (55), an integrated circuit microchip (55) and a computer diskette (44, 62, 64).

56. A system according to Claim 54, wherein said storage means of the accessed station (16, 43, 52) is associated with a bank computer system (16), a service provider computer system (40) and a telephone exchange (52).

57. A system according to Claim 46, wherein at least one said accessing station (12, 41, 50) includes a PC or computer terminal (41).

58. A system according to Claim 46, wherein at least one said accessing station (12, 41, 50) includes a mobile transceiver (50).

59. A method according to Claim 46, wherein said improvement comprises of using access codes sent directly between accessed station and accessing station by means of the Internet (42); for establishing a secure connection between a provider and a customer; comprising the steps of,

providing an active storage-memory means such as a smart card (55) mounted on a card (10) for storing one group of access codes (14) with the customer's electronic personal gadget (41, 50); said codes being sent to said customer by

means of an Internet download,

providing a specialist computerized module (46) for storing a duplicate group of access codes (14) with the provider, said group being identical to the group of codes stored in the accessing station (41, 50); means of,

providing a verification software program running on said computer for randomly choosing, requesting (challenge), and receiving a code sent (response) from the customer during establishing a secure connection,

accessing a code from the group of codes present in the accessed station (46) in a similar manner;

comparing the code received from the accessing station with the code from the accessed station, wherein a perfect match is a successful verification; and

preventing further use of said used code by the customer by means of a verification software program running on the computer automatically programmed to avoid reusing such previously used codes; means wherein,

upon failure of an initial verification, said software is automatically programmed to initiate a repetitive verification sequence until it has achieved three positive consecutive verifications in order to establish the identity of said customer or subscriber; means wherein

said software being automatically programmed for sending verification messages to advise customers and subscribers of verification needs and security breaches.

upon being exhausted of valid access codes, said defunct storage means is self replenished with fresh groups of access codes (14) through Internet downloads;

sent directly from said service provider's verification computer system (43, 46 47) into said customer's electronic communications access device (41, 50) and smartcard storage means (55).

60. A computerized code based door opening apparatus as recited in Claim 46, for accessing a safe room or high security area (60) comprising:

a user inaccessible part (accessed station) for controlling access to said safe room or high security area;

a storage means (62) within the accessed station for storing one group of access codes (14);

a storage means (64) in possession of the user for storing a duplicate group of codes (14), wherein when the user requires access to the safe room (60), storage means (64) serves as an electronic key to gain access by providing a valid code to the accessed station, said accessed station requiring an identical valid code from storage means (62) to grant access to the safe room, wherein the groups of codes are automatically replenished based upon a triggering event such that each code is used only once.

61. A system as recited in Claim 46, characterized in that upon completion of download or transfer of newly generated access codes from said spreadsheet generation means (13, 45, 57, 63) into the transit module (17, 47, 59) or storage module (15, 46, 58); a self-destruct mechanism is automatically activated by the software means to permanently remove and delete all traces of said access codes from said generator.

62/ An apparatus characterized in that defunct or damaged magnetic strips (11) on ATM cards (10) are manually changed out and replaced with new carrier strips (21).

63. A method as recited in Claim 62, said improvement including providing means

wherein new replacement magnetic strips (21) mounted on blank or dummy cards (2O), can be transferred and manually affixed onto said ATM cards (10); wherein,

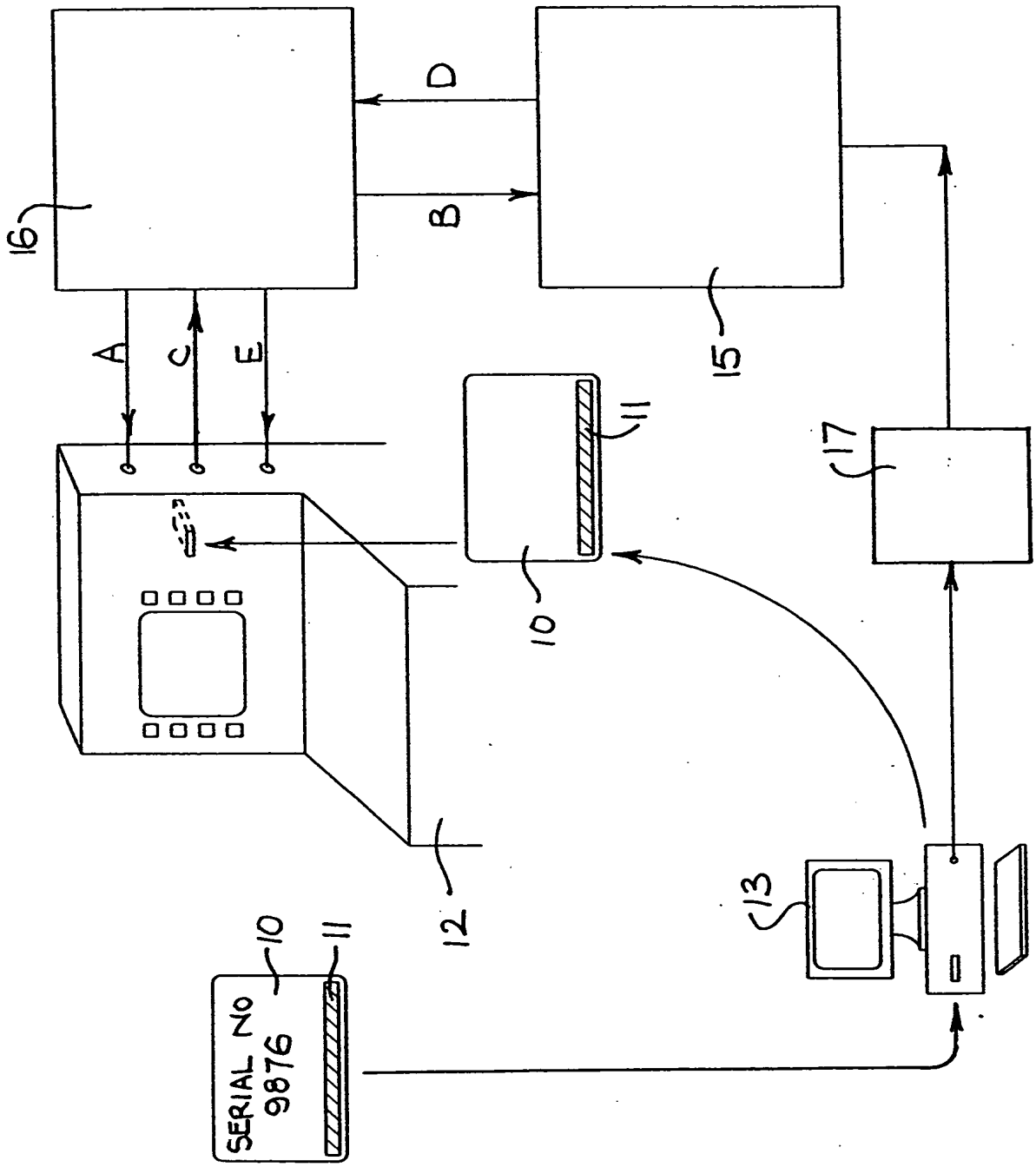
damaged smart cards (55) mounted on ATM cards can be changed out and replaced with new smartcards.

64. A method as recited in Claim 63, said improvement including means wherein damaged I.C. microchips mounted on ATM cards can be changed out and replaced with new memory chips (55).

Abstract

Improvements In Code Based Access Systems

A system including at least two stations wherein a transaction or connection between any two or more of the stations is conducted or established directly by means of an access code (14), the access code being available to an accessed station (16, 43, 52) and requiring an identical access code to be provided by an accessing station (12, 41, 50) at the time of conducting the transaction or establishing the connection such that said access codes are sent to subscribers by means of electronic communications system and the Internet (47, 48, 43, 42, 41, 44). The system is characterized in that access codes and verification messages are used in securing transactions. The system is further characterised in that the access codes is one of a plurality of codes provided to the accessed station and available to the accessing station, said access codes being generated by means of a spreadsheet generator (13, 45, 57, 63) in which a regular grid or pattern of characters and numbers are mixed in a controlled manner to produce a non repeating sequence of characters and numbers for use. The system is further characterised in that the access code is randomly selected from the plurality of codes at the time of conducting the transaction or establishing the connection, using said selected code for verification "in real time" by means of a "challenge-response" mechanism; such that no two transactions are conducted or no two connections are established with the same access codes by means of a computerized verification software (43) programmed to avoid re-using previously used access codes for conducting further transactions or for establishing further connections. The system is further characterised in that four distinct specialized modules (43, 45, 46, 47) comprising the accessed station is configured for handling a large number of customers efficiently, such that said codes are used in a repetitive "multiple strikes" verification mechanism, such that upon failure, said accessing station being barred from conducting a secure transaction or establishing a secure connection by said accessed station.



CODE NUMBER	SET
1	ABCDEF
2	1234567
3	•-••----
4	-2BT4•7
5	R2D2xZ
6	C3PO•-K
7	UCELOXX
8	7890DD
9	•-ABC123
↓100 SETS	

14

FIG 1

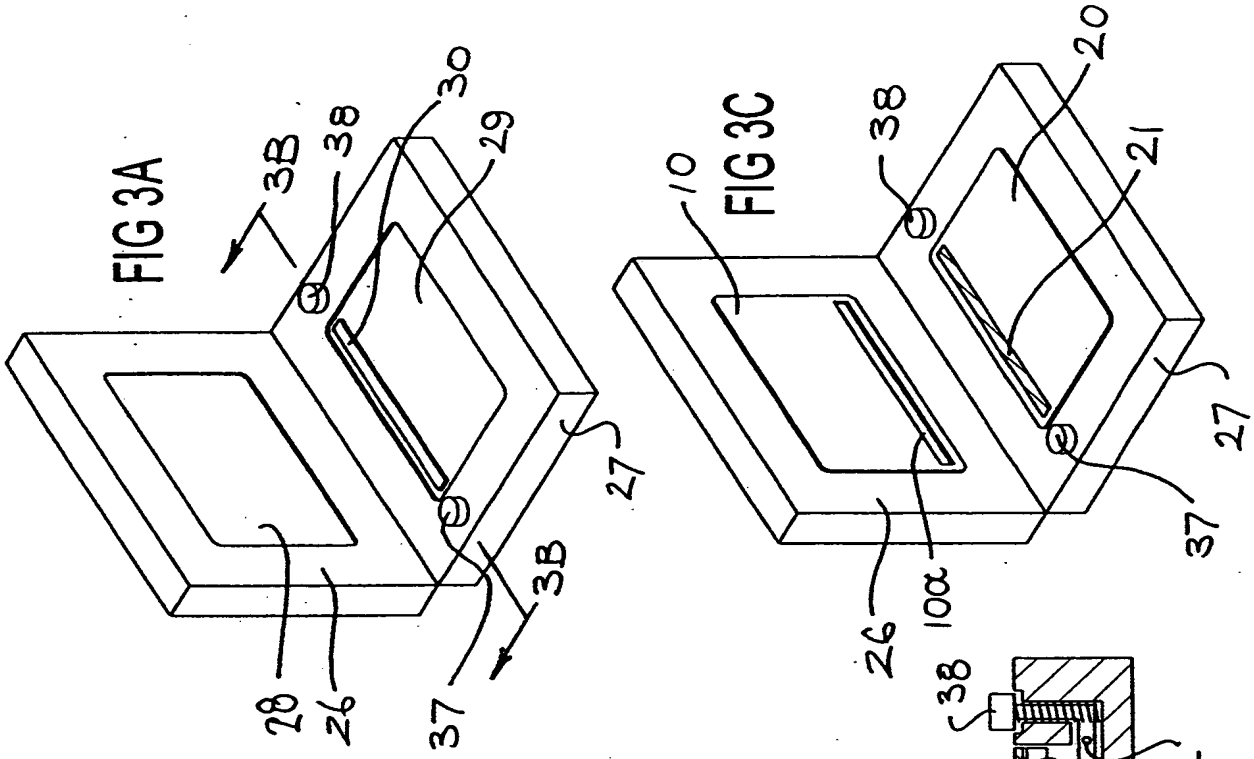
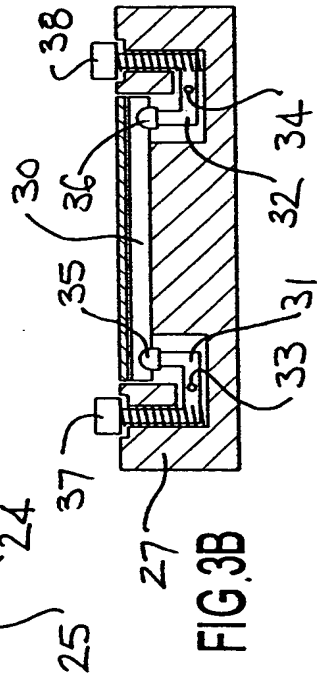
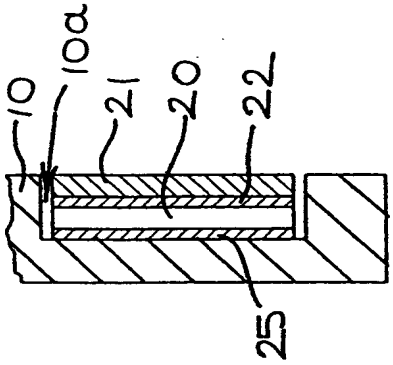
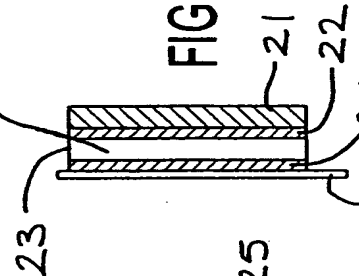


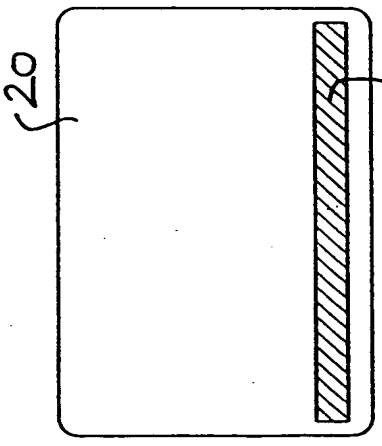
FIG 3A
3B
38
30
29
28
26
37
27
3B

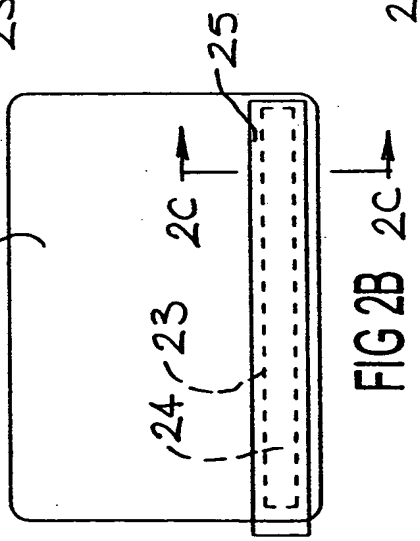
FIG 3C
10
38
20
21
27
37
26
10a


38
34
30
36
32
35
31
33
37
27
FIG 3B


10
10a
21
20
22
25
FIG 4


20
21
22
24
23
25
FIG 2C


20
21
FIG 2A


25
20
2C
2C
23
24
FIG 2B

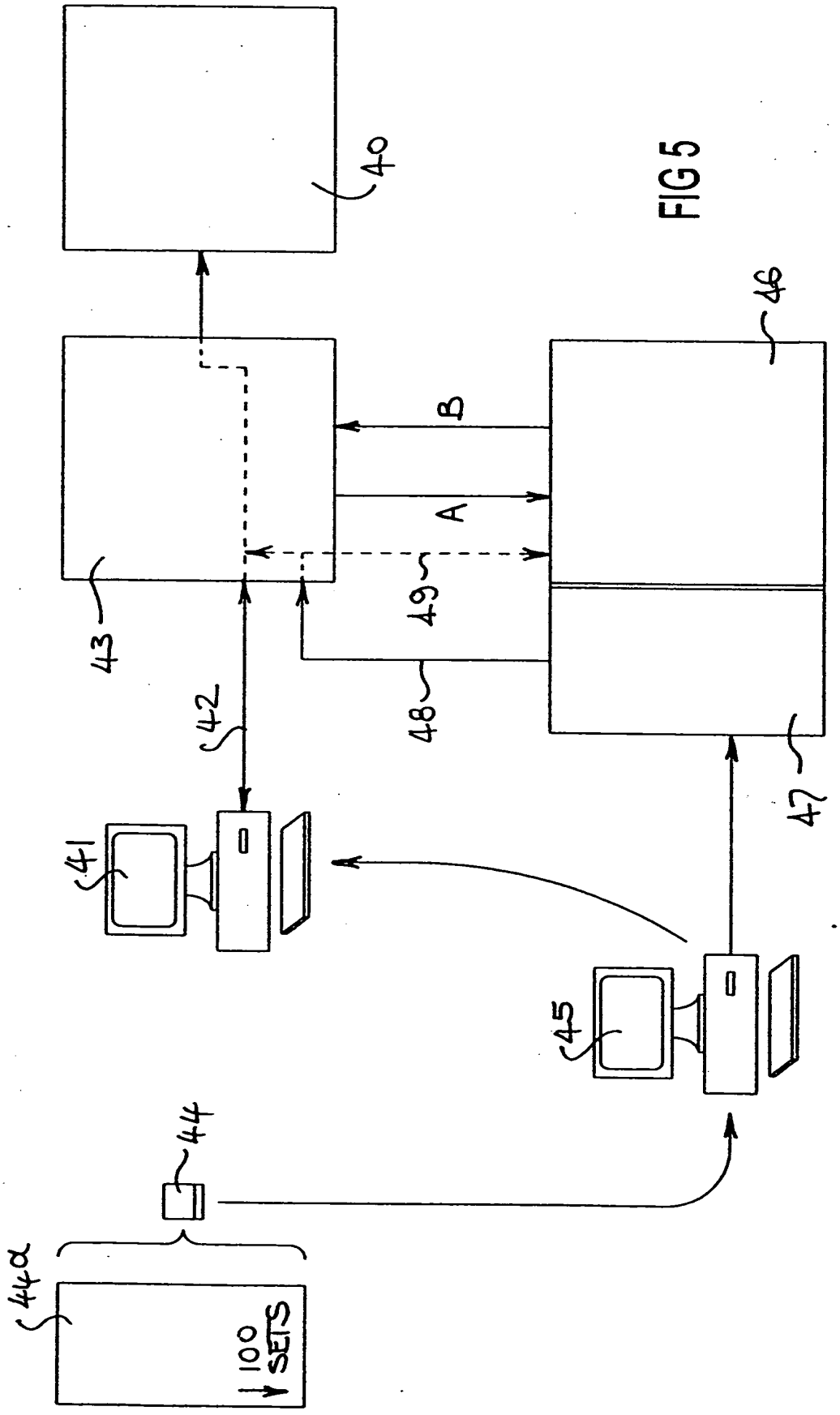


FIG 5

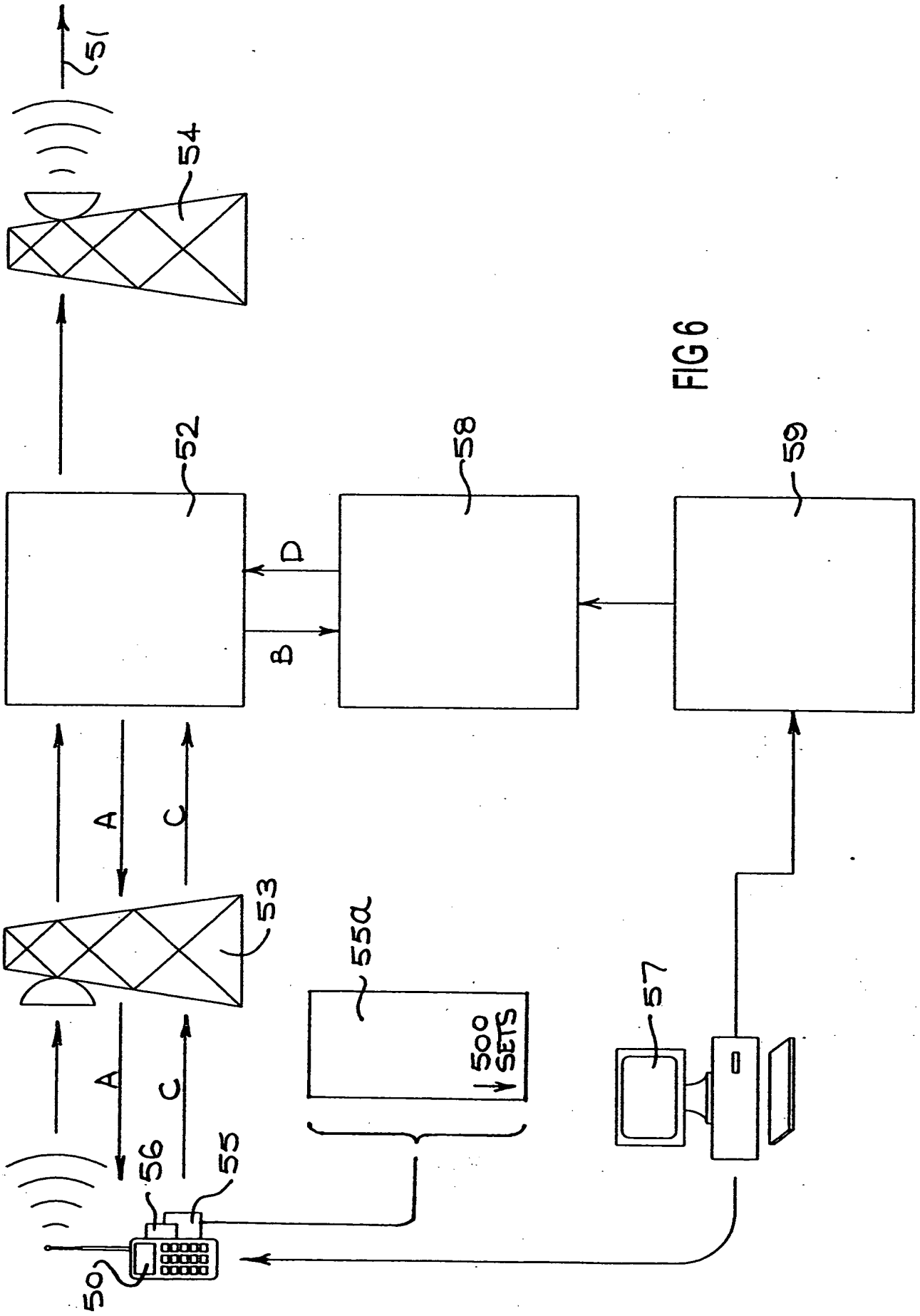


FIG 6

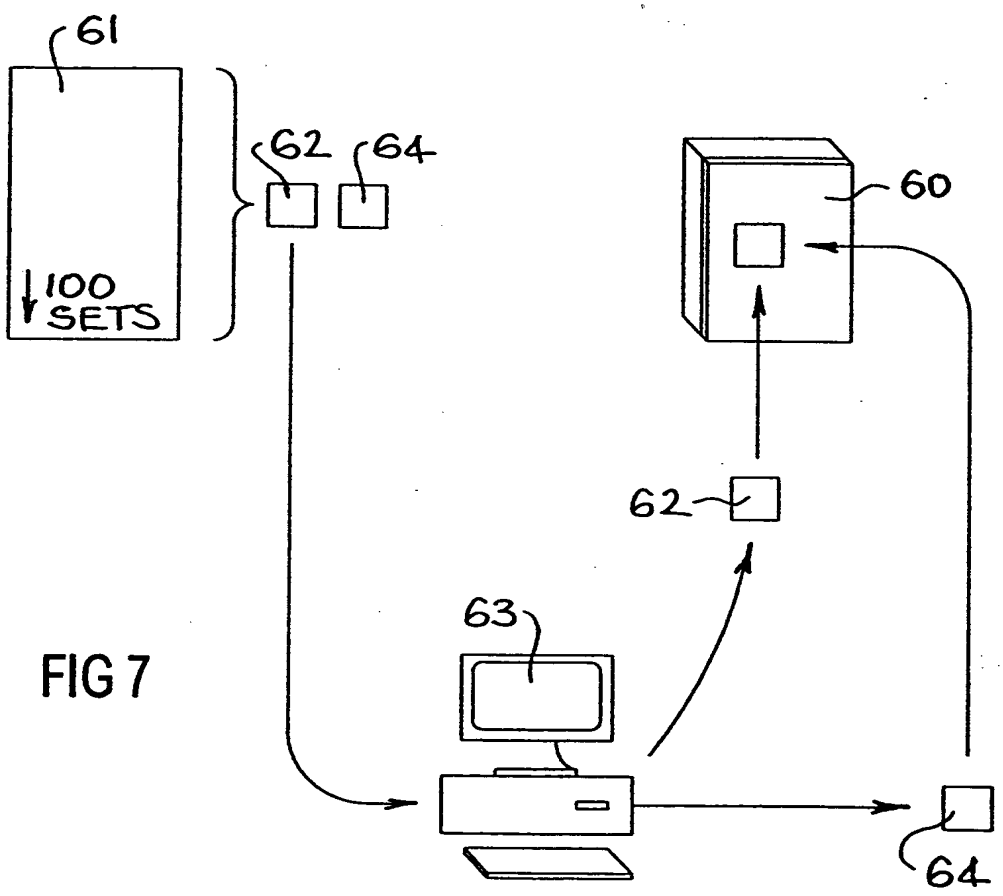


FIG 7